REMARKS

Claims 1-81 are pending and remain in the application. Claims 1, 3, 13, 15, 19, 29, 30, 32, 58, 59, 60, 69, and 78-81 have been amended. Claims 2 and 31 have been cancelled. No new matter has been entered.

The specification stands subject to objection for informalities. The specification has been amended to address the objections and to update references to commonly-assigned patent application, which have either been published or have issued since the time of the filing of this application. Further, support for the terms "encrypter," "repeater," and "programmer" can be found in the specification on page 4, lines 6-10 and page 13, line 22 to page 17, line 25. No new matter has been entered. Withdrawal of the objection is requested.

Claims 3 and 32 stand subject to objection for informalities. Claims 3 and 32 have been amended. No new matter has been entered. Withdrawal of the objection is requested.

Rejections under 35 U.S.C. § 112

Claims 59, 78, and 81 stand rejected under 35 U.S.C. § 112, second paragraph, for indefiniteness. Independent Claims 59, 78, and 81 have been amended. Support for the claim amendments can be found in the specification on page 13, line 22 to page 17, line 25. No new matter has been entered. Withdrawal of the rejection is requested.

Rejections under 35 U.S.C. § 101

Claims 1-29, 60-68, and 79 stand rejected under 35 U.S.C. § 101 because the claimed invention is directed to non-statutory subject matter. Claims 1, 60, and 79 have been amended to become statutory. Claims 2-29 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 61-68 are dependent on Claim 60 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. As the claimed invention is directed to statutory subject matter, withdrawal of the rejection is requested.

Claim 77 appears to be missing from one of the rejections, as there is no allowable subject matter. Claim 77 is the corresponding method claim of system

Claim 68, which stands rejected under 35 U.S.C. § 103 (a) as applied to U.S. Patent No. 7,027,872, to Thompson in view of U.S. Patent No. 6,442,432, to Lee. Consequently, for purposes of response, the 35 U.S.C. § 103(a) rejection as applied to Thompson and Lee is assumed to apply to Claims 4, 61, 68-70, and 77-81, as specifically discussed *infra*.

Rejections under 35 U.S.C. § 102(e) over Thompson

Claims 1-3, 5-10, 17-20, 27-29, 31, 32, 34-39, 46-49, and 56-59 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 7,027,872, to Thompson. Applicant traverses.

A claim is anticipated under 35 U.S.C. § 102(e) only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. MPEP 2131. Thompson fails to anticipate.

Claim 1 has been amended to incorporate the limitations of now-cancelled dependent Claim 2. Claim 1 now recites an external device to establish a secure connection through a short range interface with the secure key repository, to authenticate authorization to access data on the implantable medical device by securely retrieving the crypto key from the secure key repository, and to transact the data exchange session using the crypto key to authenticate the data by transitioning to a long range interface. Claim 30 has been amended to incorporate the limitations of now-cancelled Claim 31. Claim 30 now recites establishing a secure connection through a short range interface from an external source with the secure key repository, authenticating authorization to access data on the implantable medical device by securely retrieving the crypto key from the secure key repository, and transacting the data exchange session using the crypto key to authenticate the data by transitioning to a long range interface. Claim 59 now recites means for establishing a secure connection through a short range interface from an external device with the secure key repository, means for authenticating authorization to access data on the implantable medical device by means for securely retrieving the crypto key from the secure key repository, and means for transacting the data exchange session using the crypto key to authenticate the data by transitioning to a long range interface. Support for the claim amendments can

be found in the specification on page 13, line 22 to page 17, line 25. No new subject matter has been entered.

The claim amendments should not necessitate a new ground of rejection based on prior art not of record, as each of the limitations in the claim amendments were already considered and examined in the first Office action. *See* MPEP 706.07(a) ("A second or any subsequent action on the merits in any application or patent involved in reexamination proceedings should not be made final if it includes a rejection, on prior art not of record, of any claim amended to include limitations which should reasonably have been expected to be claimed" (emphasis added)).

Thompson discloses a medical data management system for variable data encryption (Col. 4, lines 40-44). A device, such as a programmer or clinician computer, receives data from an implantable medical device (Thompson, Col. 8, lines 20-26). The data is then encrypted and transmitted to a further device. Each of the devices includes an encryption engine and a decryption engine to process the data for transmission (Thompson, Col. 9, lines 16-29). Once the encryption engine receives the data, a classifier determines a type of the data, which is then output to a segregator (Thompson, Col. 7, lines 14-16). The segregator separates the data based on predetermined security levels to determine what level of encryption, if necessary, is needed (Thompson, Col. 7, lines 17-20). Upon determining the level of encryption needed, the data is encrypted and transmitted to another device (Thompson, Col. 7, Lines 23-30). A key source provides the transmitting device with an encryption key and the receiving device with a compatible decryption key (Thompson, Col. 8, lines 48-50). Thus, Thompson focuses on determining a level of encryption needed for the transmitted data.

Each device encrypts the data using an encryption engine stored on the device. Since the encryption occurs on the device that is transmitting the data, the transfer of data involves a single communication, during which the data is sent to another device, instead of a multi-step communication process, which includes authorizing access to a crypto key through a short range interface and then transferring the data by transitioning to a long range interface upon successful

authorization. The single communication of Thompson fails to support transitioning from a short range interface for access authorization to a long range interface for the data exchange session. Thus, Thompson teaches a single communication to transfer encrypted data to a device, rather than authenticating authorization to access data on an implantable medical device by securely retrieving the crypto key and transacting a data exchange session using a crypto key by transitioning to a long range interface.

Accordingly, the Thompson reference fails to describe all the claim limitations and does not anticipate. Claims 2, 3, 5-10, 17-20, and 27-29 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 31, 32, 34-39, 46-49, and 56-58 are dependent on Claim 30 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Withdrawal of the rejection is requested.

Rejections under 35 U.S.C. § 102(e) over Lee

Claim 60 stands rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,442,432, to Lee. Applicant traverses.

A claim is anticipated under 35 U.S.C. § 102(e) only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. MPEP 2131. Lee fails to anticipate.

Claim 60 has been amended to recite a short range interface device to communicate with an implantable medical device by authenticating access to a securely maintained crypto key using a short range interface; and an external device to commence a data exchange session with the implantable medical device by transitioning to a long range interface upon successful access authentication, and to transact the data exchange session using the crypto key. Support for the claim amendments can be found in the specification on page 13, line 22 to page 15, line 29. No new matter has been added.

The claim amendments should not necessitate a new ground of rejection based on prior art not of record, as each of the limitations in the claim amendments were already considered and examined in the first Office action. *See*

MPEP 706.07(a) ("A second or any subsequent action on the merits in any application or patent involved in reexamination proceedings should not be made final if it includes a rejection, on prior art not of record, of any claim amended to include limitations which should reasonably have been expected to be claimed" (emphasis added)).

Lee discloses providing data from an implantable medical device to distributed clinicians via an interface medical device (Lee, Abstract). A patient with an implantable medical device situates himself in proximity of the interface medical unit to allow the telemetry capabilities of the medical unit to obtain data (Lee, Col. 13, Lines 40-44). Once the interface medical device receives the data, an operator facilitates communication with remote medical devices and remote data communication devices via a central network (Lee, Col. 13, line 54 through page 14, line 2).

More specifically, the interface medical unit communicates with the implantable medical device through telemetry, while the interface medical unit in turn communicates with the medical devices, data communication devices, central collaboration computer, and export server through a network connection, such as a local area network or wireless area network (Lee, Col. 10, lines 43-61 and Col. 11, lines 25-44). The interface medical unit acts as a go-between for the implantable medical device and the network accessible devices. Thus, the remote medical devices and data communication devices only receive data from the implantable medical device via the interface medical device. The transfer of data includes a single communication during which the data is sent from the implantable medical device to the interface medical device through radio frequency or proximity of the implantable medical device and interface medical device (Lee, Col. 11, lines 11-24). Lee fails to establish multiple communications with the implantable medical device; one communication through a short range interface and another through a long range interface. Therefore, Lee teaches a single communication with an implantable medical device to transfer data, either through either radio frequency or close proximity, rather than communicating with an implantable medical device by authenticating access to a crypto key using

a short range interface and then commencing a data exchange session with the implantable medical device by transitioning to a long range interface.

Accordingly, the Lee reference fails to describe all the claim limitations and does not anticipate Claim 60. Withdrawal of the rejection is requested.

Rejections under 35 U.S.C. § 103(a) over Thompson and Lee

Claims 4, 33, 61, 68-70, and 78-81 stand rejected under 35 U.S.C. § 103(a) as being obvious over Thompson and further in view of Lee. Applicant traverses.

The Examination Guidelines for Determining Obviousness Under 35 U.S.C. 103 in View of the Supreme Court Decision in *KSR International Co. v. Teleflex Inc.*, 72 Fed. Reg. 57,526 (Oct. 10, 2007) ("*KSR* Guidelines"), effective October 10, 2007, control obviousness determinations and provide exemplary rationales, as incorporated in MPEP 2143. Rationale (G), which includes some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention, appears to have been applied. Three factual inquiries must be made.

First, a finding must be made that there was some teaching, suggestion, or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. MPEP 2143(G)(1).

The Thompson-Lee combination lacks a motivation to combine. "The motivation to combine may be implicit and may be found in the knowledge of one of ordinary skill in the art, or, in some cases, from the nature of the problem to be solved." Dystar Textilfarben GmbH & Co. Deutschland KG v. C.H. Patrick Co., 464 F.3d 1356, 1366 (Fed. Cir. 2006). Thompson focuses on providing "the differentiation, segregation, and classification of data at required or needed levels of security" (Thompson, Abstract). More specifically, different levels of encryption are automatically provided based on a type of data received (Thompson, Col. 5, lines 58-67). Thus, Thompson provides a solution for reducing the amount of bandwidth needed to encrypt sensitive data by

determining a type of the data and a corresponding encryption level for that type of data (Thompson, Col. 4, lines 49-Col. 5, lines 40). For example, data that is classified as less sensitive may be transmitted in unencrypted form or with minimal encryption (Thompson, Col. 5, lines 64-67). Further, each device in Thompson is equipped with an encryption engine that includes a classifier and segregator to determine the level of encryption needed for each type of data transmitted and to encrypt the data. Modifying Lee to include classification of necessary encryption would require each device to include an encryption engine with a classifier, which would hinder distributed clinician communication for those clinicians with devices not having the classifier.

In contrast, Lee focuses on providing data between distributed clinicians to enable real time communication. The Thompson and Lee references attempt to solve two different problems involving different aspects of transferring data. As such, one skilled in the art would not be motivated to combine the references. Accordingly, a teaching, suggestion, or motivation to combine Thompson and Lee has not been shown.

Next, a finding that there was a reasonable expectation of success must be made. MPEP 2143(G)(2). Claims 69 and 78-81 have been read on a combination of Rowlandson, Nappholz, and Whitehurst, but how the combination would be reasonably expected to succeed has not been explained. "The mere fact that references can be combined or modified does not render the resultant combination obvious unless the results would have been predictable to one of ordinary skill in the art." MPEP 2143.01(III) (citing *KSR International Co. V. Teleflex Inc.*, 550 U.S. __, __, 82 USPQ2d 1385, 1396 (2007)).

Further, the Thompson-Lee combination fails to teach each and every element of the claims. Claim 69 has been amended to recite maintaining a short range interface device, comprising communicating with an implantable medical device and authenticating access to a securely maintained crypto key using a short range interface. Claim 69 further recites commencing a data exchange session with the implantable medical device by transitioning to a long range interface upon successful access authentication and transacting the data exchange session

using the crypto key. Similarly, Claim 78 recites means for communicating with an implantable medical device by means for authenticating access to a securely maintained crypto key using a short range interface. Claim 78 further recites means for commencing a data exchange session with the implantable medical device by means for transitioning to a long range interface upon successful access authentication. Support for the claim amendments can be found in the specification on page 13, line 30 to page 14, line 3. No new matter has been entered.

In contrast, Thompson teaches variable encryption. A device, such as a programmer or clinician computer, receives data from an implantable medical device (Thompson, Col. 8, lines 20-26). Each of the devices includes an encryption engine and a decryption engine to process the data for transmission (Thompson, Col. 9, lines 16-29). Once the encryption engine receives the data, a classifier determines a type of the data, which is then output to a segregator (Thompson, Col. 7, lines 14-16). The segregator separates the data based on predetermined security levels to determine what level of encryption, if necessary, is needed (Thompson, Col. 7, lines 17-20). Upon determining the level of encryption needed, the data is encrypted and transmitted to another device (Thompson, Col. 7, Lines 23-30). A key source provides the transmitting device with an encryption key and the receiving device with a compatible decryption key (Thompson, Col. 8, lines 48-50). Thus, Thompson focuses on determining a level of encryption needed for the transmitted data.

Each device encrypts the data using an encryption engine stored on the device. Since the encryption occurs on the device that is transmitting the data, the transfer of data involves a single communication, during which the data is sent to another device, instead of a multi-step communication process, which includes authorizing access to a crypto key through a short range interface and transferring the data by transitioning to a long range interface upon successful authorization. The single communication of Thompson fails to support transitioning from a short range interface for access authorization to a long range interface for a data exchange session. In addition, the transfer of data fails to include multiple

communications with the implantable medical device. Thus, Thompson teaches a single communication to transfer encrypted data to a device, rather than communicating with an *implantable medical device* by authenticating access to a securely maintained crypto key using a short range interface and commencing a data exchange session with the *implantable medical device* by transitioning to a long range interface upon successful access authentication.

Moreover, Lee discloses providing data from an implantable medical device to distributed clinicians via an interface medical device (Lee, Abstract). A patient with an implantable medical device situates himself in proximity of the interface medical unit to allow the telemetry capabilities of the medical unit to obtain data (Lee, Col. 13, Lines 40-44). Once the interface medical device receives the data, an operator facilitates communication with remote medical devices and remote data communication devices via a central network (Lee, Col. 13, line 54 through page 14, line 2).

More specifically, the interface medical unit communicates with the implantable medical device through telemetry, while the interface medical unit in turn communicates with the medical devices, data communication devices, central collaboration computer, and export server through a network connection, such as a local area network or wireless area network (Lee, Col. 10, lines 43-61 and Col. 11, lines 25-44). The interface medical unit acts as a go-between for the implantable medical device and the network accessible devices. Thus, the remote medical devices and data communication devices only receive data from the implantable medical device via the interface medical device. The transfer of data includes a single communication during which the data is sent from the implantable medical device to the interface medical device through radio frequency or proximity of the implantable medical device and interface medical device (Lee, Col. 11, lines 11-24). Lee fails to establish multiple communications with the implantable medical device; one communication through a short range interface and another through a long range interface. Therefore, Lee teaches a single communication with an implantable medical device to transfer data, either through either radio frequency or close proximity, rather than communicating

with an implantable medical device by authenticating access to a crypto key using a short range interface and then commencing a data exchange session with the implantable medical device by transitioning to a long range interface.

Claims 79-81 have also been amended. Claim 79 recites a secure external device to request the crypto key from the secure server via a secure connection based on the identification of and authentication to access the implantable medical device, to receive the crypto key, to commence a data exchange session by transitioning to a long range interface upon successful access authentication with the implantable medical device, and to transact the data exchange session using the crypto key. Similarly, Claim 80 recites requesting the crypto key from the secure server via a secure connection based on the identification of and authentication to access the implantable medical device. Claim 80 further recites commencing a data exchange session by transitioning to a long range interface upon successful access authentication with the implantable medical device. Claim 81 recites means for requesting the crypto key from the secure server via a secure connection based on the identification of and authentication to access the implantable medical device. Claim 81 further recites means for commencing a data exchange session by means for transitioning to a long range interface upon successful access authentication with the implantable medical device. Support for the claim amendments can be found in the specification on page 4, lines 23 to page 5, line 6. No new matter has been entered.

In contrast, Thompson teaches variable encryption. A device, such as a programmer or clinician computer, receives data from an implantable medical device (Thompson, Col. 8, lines 20-26). Each of the devices includes an encryption engine and a decryption engine to process data for transmission to another device (Thompson, Col. 9, lines 16-29). Once the encryption engine receives the data, a classifier determines a type of the data, which is then output to a segregator (Thompson, Col. 7, lines 14-16). The segregator separates the data based on predetermined security levels to determine what level of encryption, if necessary, is needed (Thompson, Col. 7, lines 17-20). Upon determining the level of encryption needed, the data is encrypted and transmitted to another device

(Thompson, Col. 7, Lines 23-30). A key source provides the transmitting device with an encryption key and the receiving device with a compatible decryption key (Thompson, Col. 8, lines 48-50). Thus, Thompson focuses on determining a level of encryption needed for the transmitted data.

Each device encrypts the data using an encryption engine stored on the device. Since the encryption occurs on the device that is transmitting the data, the transfer of data involves a single communication during which the data is sent to another device, instead of a multi-step communication process, which includes authorizing access to a crypto key through a short range interface and then transferring the data by transitioning to a long range interface upon successful authorization. The single communication of Thompson fails to support transitioning from a short range interface for access authorization to a long range interface for a data exchange session. Thus, Thompson teaches a single communication to transfer encrypted data to a device, rather than commencing a data exchange session with an implantable medical device by transitioning to a long range interface upon successful access authentication using a short range interface.

Moreover, Lee discloses providing data from an implantable medical device to distributed clinicians via an interface medical device (Lee, Abstract). A patient with an implantable medical device situates himself in proximity of the interface medical unit to allow the telemetry capabilities of the medical unit to obtain data (Lee, Col. 13, Lines 40-44). Once the interface medical device receives the data, an operator facilitates communication with remote medical devices and remote data communication devices via a central network (Lee, Col. 13, line 54 through page 14, line 2).

More specifically, the interface medical unit communicates with the implantable medical device through telemetry, while the interface medical unit in turn communicates with the medical devices, data communication devices, central collaboration computer, and export server through a network connection, such as a local area network or wireless area network (Lee, Col. 10, lines 43-61 and Col. 11, lines 25-44). The interface medical unit acts as a go-between for the

implantable medical device and the network accessible devices. Thus, the remote medical devices and data communication devices only receive data from the implantable medical device via the interface medical device. The transfer of data includes a single communication during which the data is sent from the implantable medical device to the interface medical device through radio frequency or proximity of the implantable medical device and interface medical device (Lee, Col. 11, lines 11-24). Lee fails to establish access authentication through a short range interface and then to transfer the data through a long range interface based on a successful access authentication. Therefore, Lee teaches communication through either radio frequency or close proximity, rather than commencing a data exchange session with an implantable medical device by transitioning to long range interface upon successful access authentication using a short range interface.

Finally, additional findings must be made based on *Graham* factual inquiries, as necessary, in view of the facts of the case under consideration, to explain a conclusion of obviousness. MPEP 2143(G)(A). No further *Graham* factual findings were made.

"If any of [the three] findings cannot be made, then this rationale cannot be used to support a conclusion that the claim would have been obvious to one of ordinary skill in the art." MPEP 2143(G). Therefore, lacking sufficient findings, the combination of Thompson and Lee fail to render independent Claims 69 and 78-81 obvious. Claim 4 is dependent upon Claim 1 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 33 is dependent on Claim 30 and is patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claim 61 is dependent upon Claim 60 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 68-70 are dependent upon Claim 69 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Withdrawal of the rejection is requested.

Rejections under 35 U.S.C. § 103(a) over Thompson, Lee, and Eckmiller

Claims 11-16, 40-45, 62, 63, 65-67, 71, 72, and 74-76 stand rejected under

35 U.S.C. § 103(a) as being unpatentable over Thompson and Lee and further in view of U.S. Patent No. 6,493,587, to Eckmiller et al ("Eckmiller"). Applicant traverses the rejection.

Claims 11-16 are dependent on Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 40-45 are dependent on Claim 30 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 62, 63, and 65-67 are dependent on Claim 60 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Claims 71, 72, and 74-76 are dependent on Claim 69 and are patentable for the above-stated reasons, and as further distinguished by the limitations recited therein. Withdrawal of the rejection is requested.

Rejections under 35 U.S.C. § 103(a) over Thompson and Wheeler

Claims 21-26, 50-55, 64, and 73 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Thompson, and further in view of U.S. Patent Application Publication No. 2002/00106913, to Wheeler et al. ("Wheeler"). Applicant traverses.

Claims 21-26 are dependent upon Claim 1 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claims 50-55 are dependent upon Claim 30 and are patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 64 is dependent upon Claim 60 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Claim 73 is dependent upon Claim 69 and is patentable for the above-stated reasons, and as further distinguished by the limitations therein. Withdrawal of the rejection is requested.

The prior art made of record and not relied upon has been reviewed by the applicant and is considered to be no more pertinent than the prior art references already applied.

Further consideration and examination of the application are respectfully requested. Claims 1-81 are believed to be in a condition for allowance. Entry of the foregoing amendments is requested and a Notice of Allowance is earnestly

solicited. Please contact the undersigned at (206) 381-3900 regarding any questions or concerns associated with the present matter.

Respectfully submitted,

Dated: March 4, 2008

By: _____
Krista A. Wittman, Esq.
Reg. No. 59,594

Cascadia Intellectual Property
500 Union Street, Suite 1005
Seattle, WA 98101

Telephone: (206) 381-3900
Facsimile: (206) 381-3999

OA Resp